Phishing

Overall Classification of this Briefing is UNCLASSIFIED

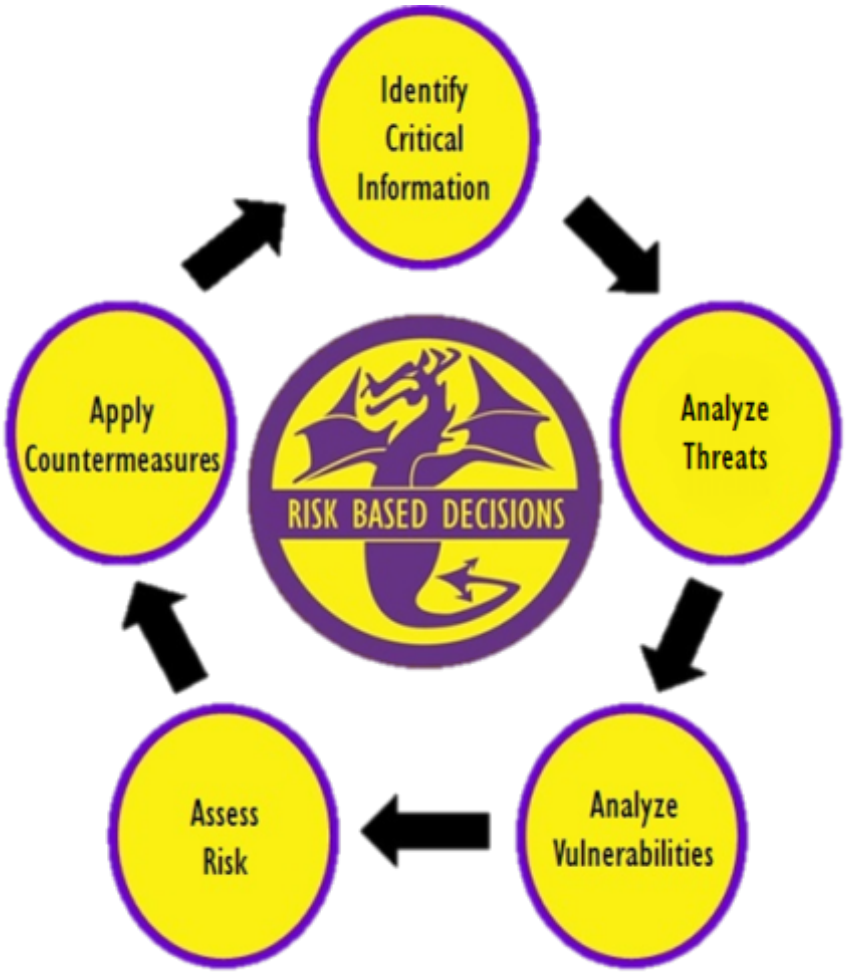
Overview

- OPSEC Overview
- What is Phishing
- IRS and Phishing
- Spear Phishing
- Whaling, Vishing, Smishing
- Identification of attack and how to protect against
- NOST Contact Info

OPSEC@navy.mil
Http://www.navy.mil/ah_online/OPSEC/index.asp
Facebook.com/NavalOPSEC
@NavalOPSEC
757-417-7100

Operations Security

- **A 5 step process that …**
  - Identifies, controls and protects sensitive, critical unclassified information about a mission, operation or activity
  - Assesses potential threats, vulnerabilities, and risk
  - Utilizes countermeasures to mitigate an adversary's effectiveness against a friendly operation



Phishing

- **Phishing is an illegal activity using social engineering techniques to fraudulently solicit sensitive information or install malicious software.**
- **Objective is to gain knowledge of sensitive information**
  - Usernames/passwords
  - Personal information
  - Military operations
  - Financial information

Characterized by a lure, hook, and catch

The Lure

- The lure is an enticement delivered through email. The email contains a message encouraging the recipient to follow an included hypertext link. The hyperlink often masks a spoofed uniform resource locator (URL) of a legitimate website.

The Hook

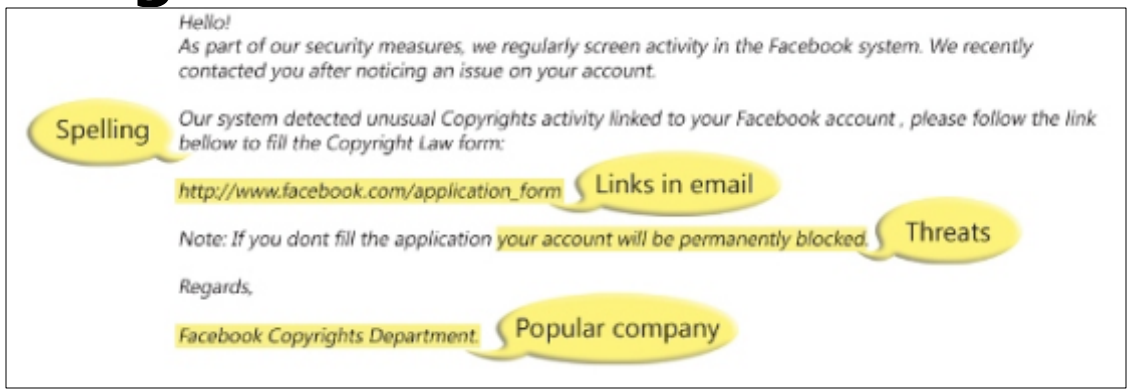
- The hook is a malicious website designed to look and feel like a legitimate website. The authentic-looking website asks the victim to disclose privacy-related information, such as user identification and password. Often the hook is an obfuscated URL that is very close to one the victim finds legitimate and is really a site under the attacker's control.

The Catch

- The catch is when the originator of the phishing message uses the information collected from the hook to masquerade as the victim and conduct illegal financial transactions.

Phishing

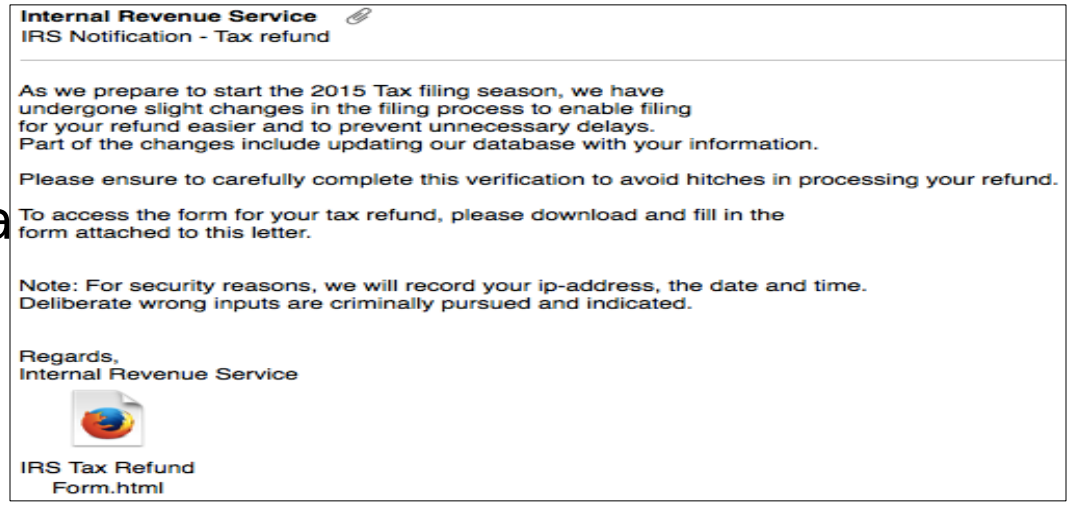
- **Phishing: attempts, via email, to acquire personal information from an Internet user by pretending to be a credible source**


Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.
Spelling
Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:
http://www.facebook.com/application_form
Links in email
Note: If you dont fill the application your account will be permanently blocked.
Threats
Regards,
Facebook Copyrights Department.
Popular company

- **Indicators:**
  - Spelling errors
  - Links in the email (malicious)
  - Communicated threats
  - Will be from a prominent business or company

Internal Revenue Service

- **Phishing Remains on the IRS "Dirty Dozen" List of Tax Scams for the 2016 Filing Season**
- **The IRS does not initiate taxpayer communications through email**
- **Scammers send email claiming to be from IRS**
- **Requests that you click on a link to fill out a form**
  - Malicious link
  - Form asks for persona information


Internal Revenue Service
IRS Notification - Tax refund
As we prepare to start the 2015 Tax filing season, we have undergone slight changes in the filing process to enable filing for your refund easier and to prevent unnecessary delays. Part of the changes include updating our database with your information.
Please ensure to carefully complete this verification to avoid hitches in processing your refund.
To access the form for your tax refund, please download and fill in the form attached to this letter.
Note: For security reasons, we will record your ip-address, the date and time. Deliberate wrong inputs are criminally pursued and indicated.
Regards,
Internal Revenue Service
IRS Tax Refund Form.html

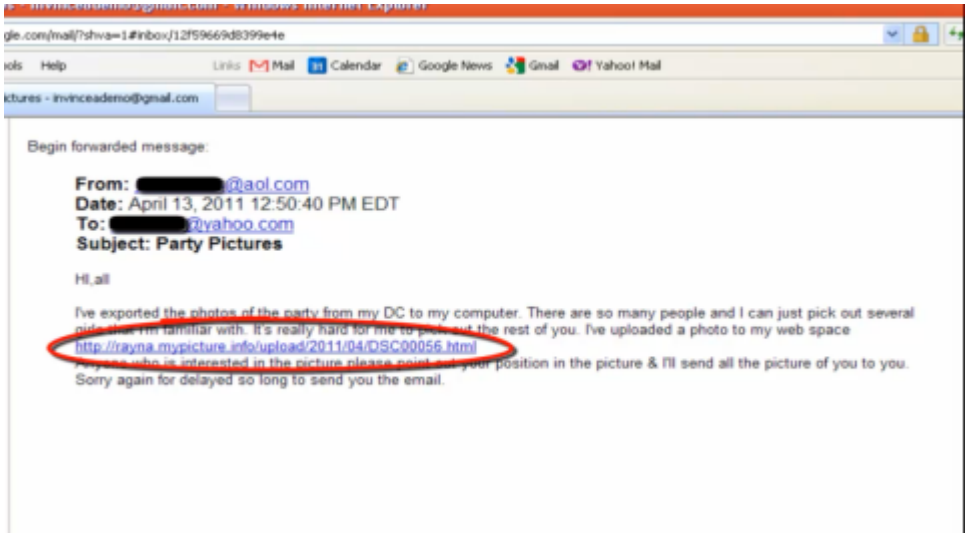
Spear Phishing

- **Information is collected on a person and then used to convince the individual that the sender is a legitimate entity that "knows"**

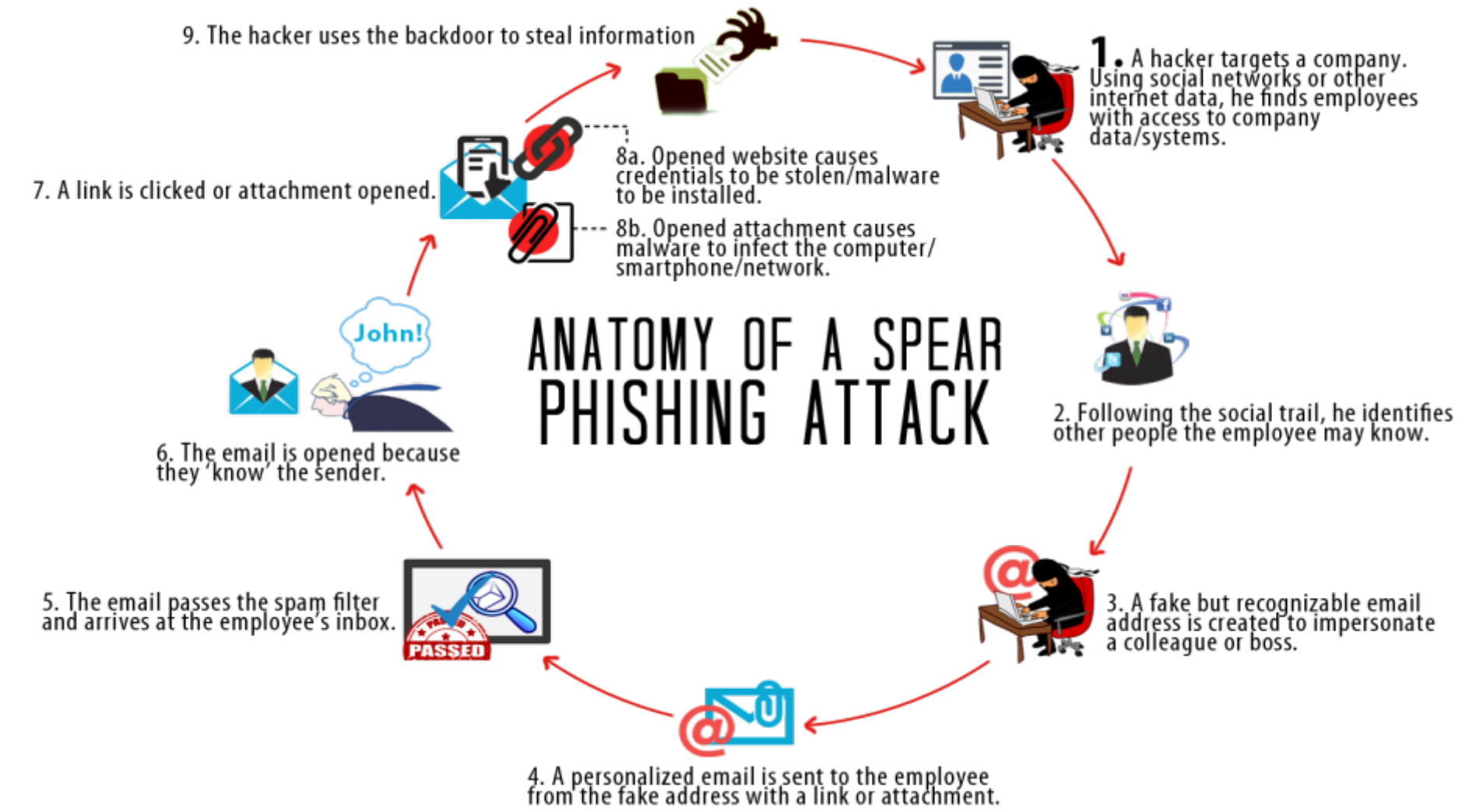
95%

"95% of all attacks on enterprise networks are the result of successful spear phishing"

Source: Allan Paller, Director of Research - SANS Institute


Begin forwarded message:
From: [redacted]@aol.com
Date: April 13, 2011 12:50:40 PM EDT
To: [redacted]@yahoo.com
Subject: Party Pictures
Hi,all
I've exported the photos of the party from my DC to my computer. There are so many people and I can just pick out several
http://rayna.mypicture.info/upload/2011/04/DSC00056.html
Sorry again for delayed so long to send you the email.

Spear Phishing

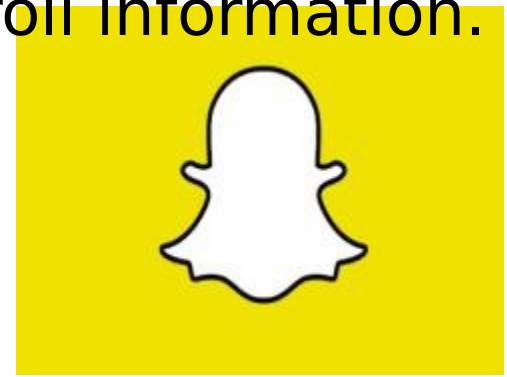

ANATOMY OF A SPEAR PHISHING ATTACK
1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.
2. Following the social trail, he identifies other people the employee may know.
3. A fake but recognizable email address is created to impersonate a colleague or boss.
4. A personalized email is sent to the employee from the fake address with a link or attachment.
5. The email passes the spam filter and arrives at the employee's inbox.
PASSED
6. The email is opened because they 'know' the sender.
John!
7. A link is clicked or attachment opened.
8a. Opened website causes credentials to be stolen/malware to be installed.
8b. Opened attachment causes malware to infect the computer/ smartphone/network.
9. The hacker uses the backdoor to steal information

Whaling

- Phishing attempt that is purported to come from a senior employee of an organization
- Any links are most likely malicious

From: United States District Court [mailto:subpoena@uscourts.com]
Sent: Monday, April 14, 2008 8:12 AM
To:
Subject: Subpoena in case #24-157-PVM
UNITED STATES DISTRICT COURT
Issued by the
UNITED STATES DISTRICT COURT
Issued to: Panos Anastassiadis
Cywellance, Inc.
703-351-1000
SUBPOENA IN A CIVIL CASE
Case number: 24-157-PVM
United States District Court
YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.
Place: United States Courthouse
880 Front Street
San Diego, California 92101
Room: Grand Jury Room
room 4217
Issuing officers name and address: O'Melveny & Meyers LLP; 400 South Hope Street, Los Angeles,
Please download the entire document on this matterfollow this link and print it for your record.
This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer on behalf of the court.
Download includes a keystroke logger virus

- March 2016: Snapchat's payroll department was targeted by an isolated email phishing scam in which a scammer impersonated a CEO and asked for employee payroll information.



Vishing

- **Scam that attempts to gain personal knowledge via phone call**
- **Imitates legitimate business**
- **Usually warns victim of fraudulent use of credit card or bank account**
  - Requests banking information

I'll need your card details
Your payment hasn't gone through
Please confirm your account password
I'm one of your suppliers

Smishing

- **Scam that uses text messages to trick victims into downloading a Trojan horse or virus onto their mobile device**

- **May prompt victim to call a number**
  - Personal information (bank, credit card, etc) will be requested

AT&T 3G
9:43 AM
Messa...(23)
1 (410) 000-003
Edit
MSG:WellsFargo Message! we are unable to complete your request online.Account locked. Please call us at
(Con't) 2 of 2
1-800-378-76
for further
Text Mess
Dear Walmart shopper, Congratulations you have just won a $1000 Walmart Gift Card. Click here to claim your gift.
www.WmartClick.com
(cancel: reply STOP)

Identifying a phishing scam

- **Phishing scams have easily recognizable characteristics**
  - Spelling and punctuation errors
  - Using threats to get people to give up their personal information
  - Enticing subject lines
  - Include a link to a web site requesting personal information

I HAVE A NEW HOBBY. IT'S CALLED PHISHING.
www.dilbert.com scottadams@aol.com
I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFOR-MATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.
8-12-05 ©2005 Scott Adams, Inc./Dist. by UFS, Inc.
Dear Customer,
This is your bank. We forgot your social security number and password. Why don't you send them to us so we can protect your money.
Sincerely,
I. B. Banker
LOOKS LEGIT.
© Scott Adams, Inc./Dist. by UFS, Inc.

Protect yourself

- **Do not open emails from someone you don't know**
- **Your bank will never email you for personal information**
  - Visit or call the bank if you have doubt about your account
- **Never unsubscribe from spam emails**
  - Mark as spam and delete

Summary

- OPSEC Overview
- What is Phishing
- IRS and Phishing
- Spear Phishing
- Whaling, Vishing, Smishing
- Identification of attack and how to protect against
- NOST Contact Info

Questions

JEB – Little Creek (Bldg 1126)

2555 Amphibious Drive

Virginia Beach, VA 23459-3225

OPSEC@Navy.mil

757-417-7100

Naval OPSEC App

Collaboration at Sea

www.navy.mil/ah_online/OPSEC/index.asp
www.navy.mil/local/OPSEC

Facebook.com/NavalOPSEC

@NavalOPSEC

Youtube.com/USNOPSEC